# Cassandra Crossing/ Tor, lezione di teoria—2

(97)—Proseguono gli approfondimenti su Tor e le tecnologie di anonimizzazione, dalla teoria alla pratica. A parlarne è un esperto…

---

**Cassandra Crossing/ Tor, lezione di teoria—2**

Figure 1:

*(97)—Proseguono gli approfondimenti su Tor e le tecnologie di anonimizzazione, dalla teoria alla pratica. A parlarne è un esperto d'eccezione: Marco Calamari. Siamo al secondo round.*

26 ottobre 2007—Qualche settimana fa la prima lezione di guida di Tor è stata accolta con interesse dai miei 23 lettori; il diluvio di fatti importanti accaduti in questi giorni pero' aveva richiesto che *Cassandra Crossing* si occupasse di altri temi.

Ma ogni promessa è debito, quindi eccoci qui. Come ai tempi della scuola guida pero', lezioni pratiche vanno alternate con lezioni teoriche, quindi oggi la "lezione" sarà meno divertente perché tocca alla teoria, anzi alla teoria di base. Niente crittografia od algoritmi però, ma solo una importantissima riflessione su quello che accade realmente nel PC quando navighiamo.

La normale navigazione con un browser (useremo nuovamente Firefox come esempio) è molto più complessa di quello che sembra.

Un sacco di cose accadono "dietro le quinte" all'insaputa dell'utente che non si interessi specificamente all'aspetto informatico; un buon motivo per interessarsene almeno un po' è appunto la difesa della propria privacy. Chi naviga percepisce distintamente di avere "il controllo" della situazione, di essere l'attore del processo in corso, di essere colui che "fa succedere" le cose.Orbene, non è esattamente cosi; anzi non è proprio così.

Anzi non è affatto così.

Quando navigate, l'unico vostro ordine è quello di scegliere il prossimo link da visualizzare. A questo punto il browser apre un collegamento HTTP verso il server e richiede una certa pagina. Quello che viene trasmesso dal server al vostro browser sono una serie di informazioni che gli fanno compiere certe azioni.

Ai vecchi tempi della rete queste informazioni erano soltanto comandi HTML e file grafici. Il browser non sapeva fare altro che interpretare questi comandi, leggere le immagini e rappresentarli (il termine corretto è "renderizzare") sul vostro schermo.

Nessuna altra azione era possibile perché i vecchi browser (ricordate Mosaic?) sapevano fare solo questo. Oggi fortunatamente/purtroppo le cose sono molto cambiate. I browser sanno fare un sacco di cose in più, conoscono e possono eseguire "programmi" scritti in vari linguaggi (javascript, java e vbscript sono alcuni di essi) e possono quindi compere tutte le azioni eseguite da essi sul vostro computer; in termini tecnici possiedono interpreti o runtime interni per questi linguaggi.

Cosa significa questo? Che se la pagina che il server decide di mandarvi in risposta alla vostra richiesta contiene un programma (tecnicamente uno script od un applet) scritto in uno di questi linguaggi, esso verrà eseguito dal browser che compirà le azioni richieste dal programma stesso.

Normalmente si tratta di azioni che hanno lo scopo di visualizzare una pagina web più "ricca" di contenuti, e di renderne alcuni attivi. Gli interpreti ed i runtime dei browser normalmente hanno delle limitazioni su ciò che possono fare; ad esempio non possono passare un comando direttamente al sistema operativo, od accedere in maniera incontrollata al disco del PC. Ma gli interpreti hanno bachi che permettono di compiere anche azioni non previste, e le azioni previste possono spesso essere usate in maniera "creativamente dannosa".

Ad esempio, un applet Java può aprire una connessione ad Internet, ma solo al dominio da cui l'applet stesso è stato scaricato. Questo permette ad un server maligno di ottenere l'IP di un utente Tor; il server maligno vede arrivare la connessione da un router Tor, gli invia un applet con un identificativo casuale che, una volta eseguito dal browser, apre una nuova connessione verso il server stesso e gli invia l'identificativo. La nuova connessione viene fatta al di fuori della rete Tor e quindi rivela l'IP del PC, e l'identificativo restituito permette di associare l'IP reale alla connessione *anonima*. Voilà.

In realtà questo attacco non è più possibile con una configurazione di Tor "moderna" ma se ne possono realizzare di simili, solo tecnicamente più sofisticati. Ecco perché, se si desiderano connessioni anonime, è necessario disabilitare tutti gli interpreti interni al browser (Java e Javascript) rinunciando quindi a vedere correttamente tutte le pagine che contengono script.

E' un prezzo da pagare.Ma c'è dell'altro. I browser moderni sono scritti con una architettura a plugin, che permette di installare applicazioni scritte da terze parti dentro il browser stesso. Queste applicazioni, senza aver bisogno di script inviati dal server, possono eseguire tutte le azioni che desiderano, limitate solo da quelle ammesse dal browser. Esempi di plugin che probabilmente tutti possiedono nel proprio browser sono Flashplayer, Realplayer, Shockwave, Quicktime, Media Player.

Tutti questi plugin possono contattare il server di origine od un altro server a piacere, molti di essi possono anche installare legalmente ulteriori applicazioni arbitrarie nel vostro browser. Vi sembra impossibile? Allora dovreste provare a leggere gli accordi di licenza che approvate durante l'installazione o quando comprate il sistema operativo!

Ma lasciamo perdere questo aspetto perché il discorso richiederebbe non un articolo ma una serie di articoli a parte. Facciamo solo un paio di esempi.

Il plugin, quando eseguito, si collega normalmente con un server dell'azienda che lo produce per verificare la presenza di aggiornamenti; in questa situazione può tranquillamente (e legalmente) trasmettere dati che annullano il vostro anonimato. Anche senza considerare questa funzione, il plugin usato ad esempio per visualizzare un filmato scaricato da un server puo' eseguire una richiesta di collegamento inserita nel filmato stesso, e siamo daccapo.

Questi sono solo alcuni dei motivi per i quali la navigazione con Tor deve dovrebbe essere eseguita con un browser diverso da quello normalmente usato, configurato "castrando" tutto ciò che può portare all'esecuzione di contenuti attivi scaricati dal server con cui ci colleghiamo. Quindi non solo disabilitare Java, Javascript e VBscript, ma anche cancellare tutti i plugin ed i player add-on, e lasciare solo il minimo necessario di estensioni, come ad esempio TorButton. In Firefox ad esempio, lo potete fare nel menù Tools/Add-on:
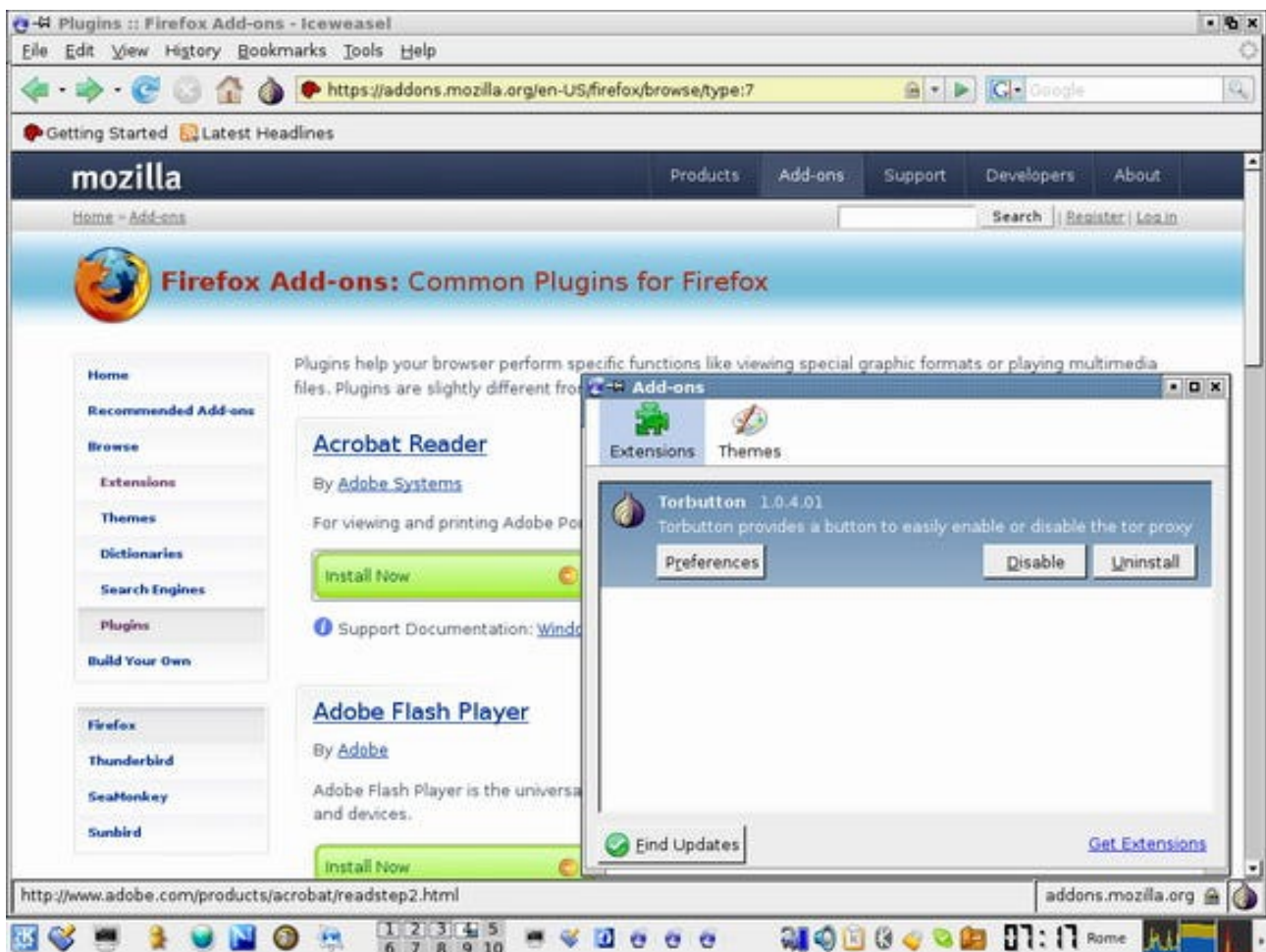
Figure 2:

in figura potete vedere sia la pagina da cui si scaricano gli add-on che la finestra da cui si gestiscono (e cancellano!)

Far questo significa ovviamente rinunciare ad una parte delle pagine e dei siti che non funzionano senza queste opzioni; è, come dicevamo, un prezzo da pagare per poter mantenere la propria privacy e/o il proprio anonimato.

Ovviamente esistono soluzioni intermedie che portano a quantità di anonimato e sicurezza intermedie, ma anche questo sarebbe un discorso amplissimo, e ne parleremo un'altra volta. Esiste, per la gioia di chi vuol faticare poco, una soluzione ad una buona parte dei problemi

suaccennati; si chiama Privoxy e moltissime installazioni di Tor per fortuna ve la installano automaticamente. Ma questa… questa è un'altra storia, per un'altra puntata.

Se Frattini, Gentiloni e soci faranno il ponte e non avranno altre alzate di ingegno, potrebbe anche essere pubblicata la prossima settimana.

---

*Originally published at punto-informatico.it.*

---

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero



By Marco A. L. Calamari on August 30, 2023.

Canonical link

Exported from Medium on August 27, 2025.